

**E-Commerce Steering Group Chair's Report on the
Outcomes of the APEC ECSG Cybersecurity Workshop,
14 August 2003, Phuket, Thailand**

The Electronic Commerce Steering Group (ECSG) held a workshop on cybersecurity on 14 August 2003. The purpose of this Workshop was to supplement the APEC work agenda on cybersecurity by addressing related issues that affect business on an individual company level, and how governments and industry can cooperate to promote a culture of security among businesses and consumers. Nine different economies and nine representatives of the private sector participated in the Workshop, and there were over 60 attendees from across the region.

Summary of the Themes

Several themes emerged from the various presentations at the workshop, including:

- Rapid development in information and communication technologies (ICTs) and increased interconnection has contributed to a general threat evolution where attacks have a global focus and where initial targets are often directed at the weakest aspects of the network – often small businesses and consumers.
- In order to address this changed risk environment, it is necessary for governments and the private sector to promote a culture of security – a cooperative approach to security that encompasses all participants who use networks and information systems, where they take appropriate steps to implement or maintain security within cyber-environments.
- In order to create a culture of security, it is necessary to conduct education and public-awareness building efforts with a specific focus on small and medium-sized enterprises (SMEs). SMEs comprise a significant percentage of economies, yet often do not realize that cybersecurity is something that they need to address. In short, they “do not know that they need to know”.
- Finally, both businesses and governments have essential roles to play in addressing cybersecurity issues and in building a culture of security.
 - Business has an obligation to raise awareness and educate employees, customers and supply chain partners about cybersecurity issues. Often industry associations can be usefully deployed to undertake this work.
 - Governments should undertake to develop partnerships with the private sector to share information and to assist in education and public outreach efforts.

Next Steps

ECSG members agree that in 2004 they will undertake the following follow-up steps to the cybersecurity workshop:

- The ECSG will circulate this report to other APEC fora addressing cybersecurity, including the APEC Telecommunications and Information Workshop Group's e-Security Task Group (eSTG). In addition, we will continue cooperation and collaboration on these issues in the future, particularly in the area of standards.
- The ECSG will continue to work with the private sector to exchange information on tools, standards, practices and policies related to cybersecurity issues in order to identify best practices in this space. This will include specifically information sharing on programs designed to provide education and public awareness building for SMEs and on outreach to consumers, including kids, and
- The ECSG will continue to work with the private sector to further address the intersection of privacy and security, with a goal of highlighting the important ways that effective, holistic and proactive security policies can significantly contribute to the work to balance effective privacy protections with the free flow of information.